SCAMADVISER

Asia Scam Report 2024

GASA
Global Anti-Scam Alliance

Little hope of loss recovery as Asia's stricken citizens bear the brunt of a US$688.42 billion scam burden

The 2024 Asia Scam Report, conducted by the Global Anti-Scam Alliance (GASA), surveyed 24,731 participants across 13 populations in the region. The findings provide an in-depth look at scam threats, the methods employed by scammers, and the responses from citizens across the region.

The report reveals wide disparities in scam recognition confidence across Asia. Citizens from China, India, Indonesia, and the Philippines expressed the highest confidence in recognizing scams, while Japan had the least confidence, with many respondents uncertain of their ability to detect fraud.

Scam frequency varies significantly across the region. Thailand and Hong Kong experience the highest rates of scam encounters, with around 90% of citizens facing scams monthly or more. In contrast, fewer than half of the populations in China & Pakistan reported encountering scams as often. Thailand & South Korea saw the largest yearly increases in scam frequency, while populations like Vietnam and Malaysia reported the most significant reductions. This could be attributed to differing levels of scam sophistication, law enforcement efforts, or public education initiatives.

AI-driven scams, especially those involving AI-generated texts and SMS messages, are gaining traction across Asia. In the Philippines, 72% of respondents believe they have been targeted by AI scams, while in Singapore, most citizens do not believe AI was involved. Vietnam and India are the most informed about AI threats, whereas Japan, Thailand, and Malaysia show the lowest awareness. This disparity in AI scam literacy highlights the need for more education to combat these new risks. Phone call scams are particularly prevalent in Thailand,

Hong Kong, and Malaysia, while text/SMS scams are common in the Philippines, South Korea, and Indonesia. Investment and shopping scams are widespread, frequently appearing among the top three scam types across the region. Identity theft, however, is the leading scam in six of the 13 surveyed populations.

Bank transfers remain the most common payment method used in scams, though electronic transfers and e-wallets are also popular. Vietnam has experienced a spike in cryptocurrency-related scams, reflecting wider trends in the adoption of digital currencies in the region.

Victims of scams in Thailand & the Philippines reported the heaviest emotional burdens, with many struggling with the psychological aftermath of their experiences. In contrast, the Japanese and Taiwanese reported the least emotional impact, potentially due to cultural differences or more stable systems for addressing scams.

A significant proportion of scams are completed within minutes, making them difficult to detect and prevent. Although most Asians realize they've been scammed on their own, the media outlets plays a key role in raising awareness, particularly in Thailand & Vietnam.

Scams have eroded trust in the Internet across Asia, particularly in the Philippines and Thailand. Conversely, citizens in China and Taiwan reported the least loss of trust. While the police are the primary destination for reporting scams across all 13 populations, uncertainty about where to report and doubts about the effectiveness of reporting are widespread. National reporting websites are popular in China, Hong Kong, Taiwan & South Korea, but other populations lag behind in offering easy access to scam reporting platforms.

China, Singapore, and South Korea lead in full recovery of scam losses, while victims in Hong Kong and Pakistan are least likely to recover their funds. Over a quarter of citizens in South Korea, Indonesia, Pakistan, Thailand, and Singapore believe no one will reimburse their losses. Asians think they should be refunded by the platform used by scammers, the website host/provider, or banks.

The report also highlights the prevalence of money muling—a scheme in which individuals unknowingly aid criminals by transferring stolen funds. Alarmingly, 1-in-5 Indians and Pakistanis admitted they might consider engaging in such schemes, while Taiwan's citizens are the least likely to be involved.

Finally, based on the responses received from the 24,731 people surveyed, we have estimated the total economic impact to the 13 populations surveyed in the 2024 Asia Scam Report to be a staggering US$688.42 billion. The findings show a need for region-wide collaboration on education, law enforcement, and public reporting mechanisms to mitigate the threat of scams in Asia.

Jorij Abraham
Managing Director

Sam Rogers
Director of Marketing

The rapid rise of real-time payments (RTP) across Asia has transformed how we move money. With RTP, individuals and businesses can transfer funds instantly, making transactions faster and more convenient. However, scammers are increasingly exploiting the fact that RTP transactions cannot be reversed, leading to a surge in financial fraud.

The Challenges of Fighting Fraud in Real-Time

RTPs have revolutionized money transfers, enabling instant transactions between accounts. However, once an RTP is made, it cannot be reversed. Fraudsters exploit this speed, transferring stolen funds across accounts in minutes, making it extremely difficult for financial institutions to trace and recover the money. One of the most prevalent types of fraud within RTP systems is Authorized Push Payment (APP) fraud. In this scam, victims are tricked into authorizing payments to fraudsters. Because these transactions are "authorized" by the account holder, financial institutions are often unable to detect these as fraudulent and reimburse victims, highlighting a gap in consumer protection.

APP fraud is a global challenge, particularly affecting populations like the UK, US, India, Brazil, and Australia. Scammers use advanced techniques, such as phishing, deepfake videos, and AI-powered voice simulations, to deceive victims into transferring funds. From the perspective of the financial institution, these transactions appear legitimate, making them difficult to detect and prevent.

Case Study: UK and Singapore

To protect consumers from rising scams, regulators in the UK and Singapore are introducing frameworks that shift liability. In the UK, the Payment Systems Regulator (PSR) is set to implement a liability-sharing system requiring both sending and receiving financial institutions to share responsibility for reimbursing APP fraud victims. This forces financial institutions to enhance fraud prevention efforts and collaborate more across the industry.

Singapore's Monetary Authority (MAS) is implementing a similar Shared Responsibility Framework (SRF), which distributes accountability for digital payment fraud among banks, payment service providers, and telcos. Given the high volume of fraud originating from telecom channels, the SRF also requires cooling-off periods and real-time alerts to prevent fraud.

These models signal a shift in how the ecosystem addresses scam liability. While they offer greater consumer protection, they also increase the responsibility on financial institutions and telecom providers to prevent and respond to fraud. This shift could pave the way for social media companies and others to be included in similar regulatory frameworks.

Evolving Fraud Prevention

As fraudsters become more skilled at exploiting RTP vulnerabilities, the need for a multi-layered fraud prevention approach grows. This involves detecting and preventing scams at all stages—from account creation to transactions. One promising approach is using AI and data insights, such as transaction patterns, behavioral biometrics, and identity verification, to detect fraud early. Since financial institutions only see within their own systems, they must collaborate across organizations to share real-time information about suspicious transactions at a network level.

In the UK, Mastercard partnered with major banks to implement an AI-based network-level solution to predict and prevent real-time payment fraud. Since early 2023, the solution has helped 11 UK banks stop scam payments before the funds leave the victim's account. By scanning multiple transaction data points, the system provides a real-time risk score to the sender's bank. PSR data from 14 banks showed a 12% reduction in the total value of APP scams from £389m ($514m) to £341m ($450m) in 2023. In September 2024, Mastercard announced enhancements providing receiving banks with "inbound risk" alerts within seconds, helping them detect payments headed for mule accounts used by fraudsters. This AI intervention, operating at millisecond speed, has drawn interest from law enforcement & banks worldwide.

Conclusion

The growth of RTP in Asia presents opportunities and challenges, particularly in fraud prevention. Lessons from the UK & Singapore suggest that regulatory frameworks across Asia are evolving to hold financial institutions accountable for protecting consumers from scams. As digitalization accelerates, it is essential for fraud prevention systems to advance. AI and machine learning will be key tools in combatting the rise in scams.

Rajat Maheshwari
Chair, GASA Singapore
Vice President, Mastercard

ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its AI-powered Anti-Scam Intelligence (ASI). ScamAdviser provides real-time detection of suspicious activity and scam prevention for websites, calls, messages, and online platforms. With the world's largest scam database, ScamAdviser partners with over 400 organizations to protect more than 1 billion consumers worldwide, helping people confidently navigate the digital world. In this interview, Aaron Chiou, Product Director of ScamAdviser, will describe the current state of scams in Asia and the advanced strategies needed for enterprises to protect consumers.

How significant has the issue of scams become in Asia?

Scams are rising across Asia, with varying levels of exposure and confidence in detecting scam. South Korea and Thailand have reported a notable increase in scam attempts over the past year, while Vietnam and Malaysia have seen a decline. Citizens in China, India, Indonesia, and the Philippines are generally more confident in their ability to detect scams, while those in Japan and South Korea report lower levels of confidence, underscoring the urgent need for better scam detection tools and public education.

Over 50% of citizens in most Asian populations face monthly scams, with Hong Kong and Thailand's exposure rates above 90%. This highlights the need for coordinated efforts to strengthen protections. Given the varied scam activity across populations, a one-size-fits-all approach is inadequate. Regions with rising scam attempts require stronger preventive measures, while those with declining activity can build on recent successes.

Which scams have trended in Asia recently?

Many Asians are becoming more aware of AI's role in creating deceptive content, such as emails, messages, and SMS. For example, 72% of Filipinos believe AI will play a larger role in SMS scams. While Vietnam shows greater awareness of AI threats, Japan, Thailand, and 65% of Singaporeans report lower understanding or doubt of AI's involvement.

Phone and SMS scams remain the most common channel for scams, with identity theft leading scam types, followed by investment scams. Bank transfers are the primary payment method, though e-wallet and cryptocurrency usage is also rising. As AI-scams increase, raising public awareness and improving detection methods are more urgent than ever, highlighting the need for faster responses and stronger preventive measures.

What action has been taken by the government and other organizations to protect consumers from scams? Any best practices from which we can learn?

Governments, telecom companies, and digital platforms should actively work to protect consumers. Governments have launched websites to help identify trustworthy links and report suspicious domains, providing real-time alerts and safety advice. Telecom providers offer apps to detect and block scam calls and SMS, while platforms track malicious domains using scam databases to block dangerous websites. These efforts are enhanced through collaboration with TrustTech providers such as ScamAdviser, offering real-time anti-scam solutions. Best practices include regularly updating scam databases, using AI to block fraud, and fostering multi-sector collaboration to stay ahead of emerging threats.

What further actions could give consumers the upper hand in fighting scams?

Many victims experience both financial losses and emotional distress, especially in Thailand and the Philippines, where trust in online platforms has declined. While many report scams to the police, others refrain due to uncertainty or feeling it's not their responsibility.

Governments must lead by partnering with businesses to provide anti-scam education and encourage reporting. Platforms and financial institutions should proactively protect users, while collaboration with TrustTech providers is key to safeguarding consumers and maintaining brand trust. A united public-private effort is essential to counter the growing threat of AI-driven and digital scams.
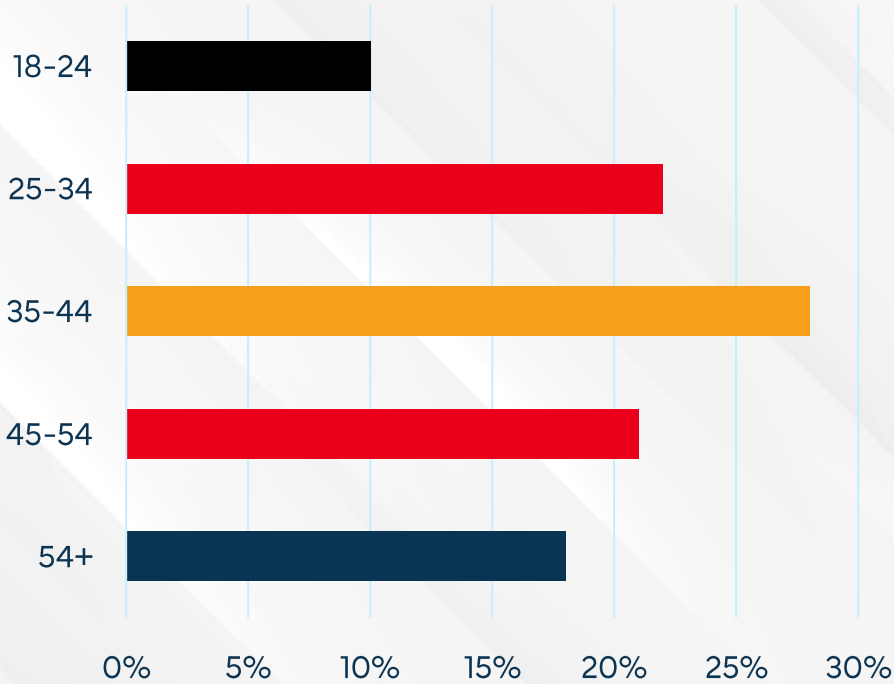
Aaron Chiou
Product Director

SCAMADVISER

24,731 people from 13 populations participated in the Asia Scam Report

SCAMADVISER

GASA Global Anti-Scam Alliance

Gender

58%

42%

Age Range

- 18-24
- 25-34
- 35-44
- 45-54
- 54+

0% 5% 10% 15% 20% 25% 30%

Education

50%
45%
40%
35%
30%
25%
20%
15%
10%
5%
0%

- middle school
- high school
- vocational
- university
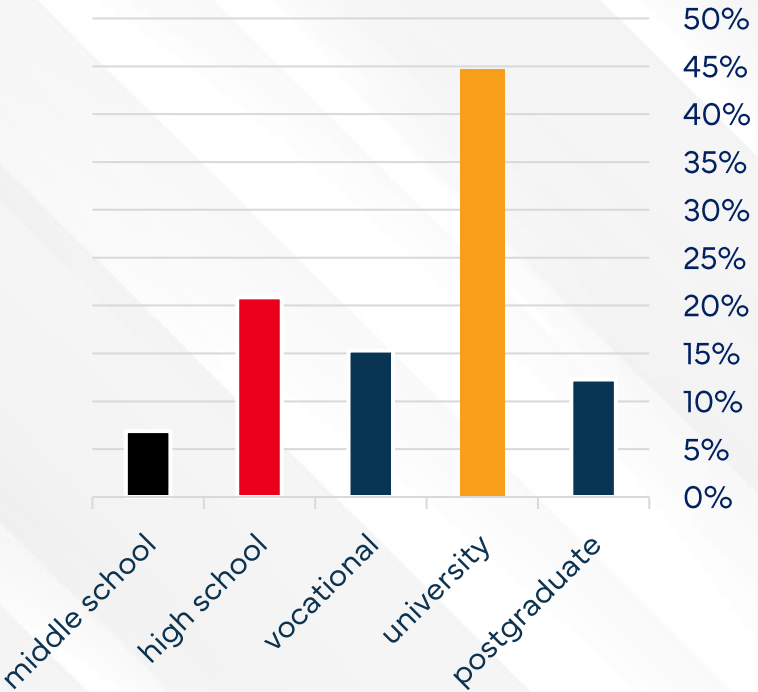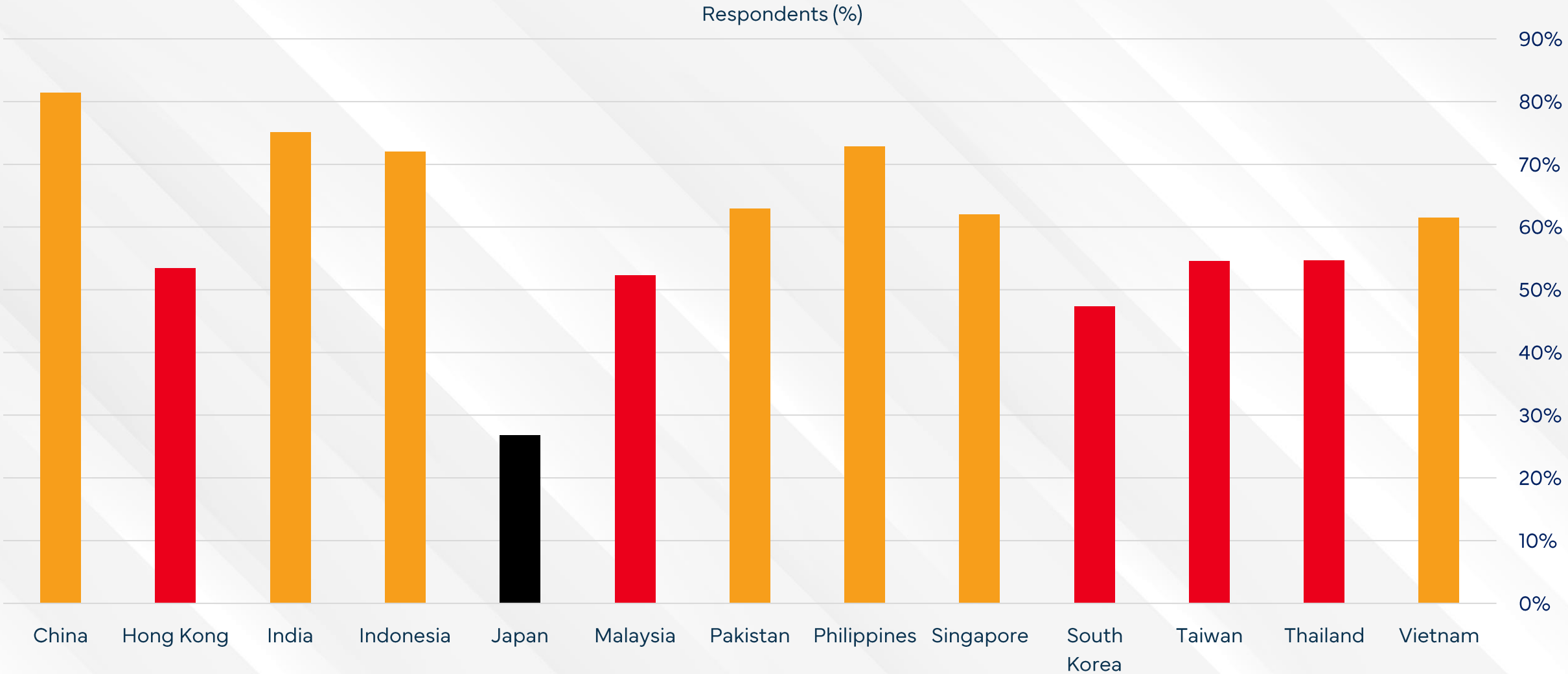- postgraduate

The citizens of China, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Philippines, Singapore, South Korea, Taiwan, Thailand, and Vietnam, tended to be a male aged 35–44 with a university education.

The Japanese have the least confidence in their ability to recognize scams

SCAMADVISER

GASA
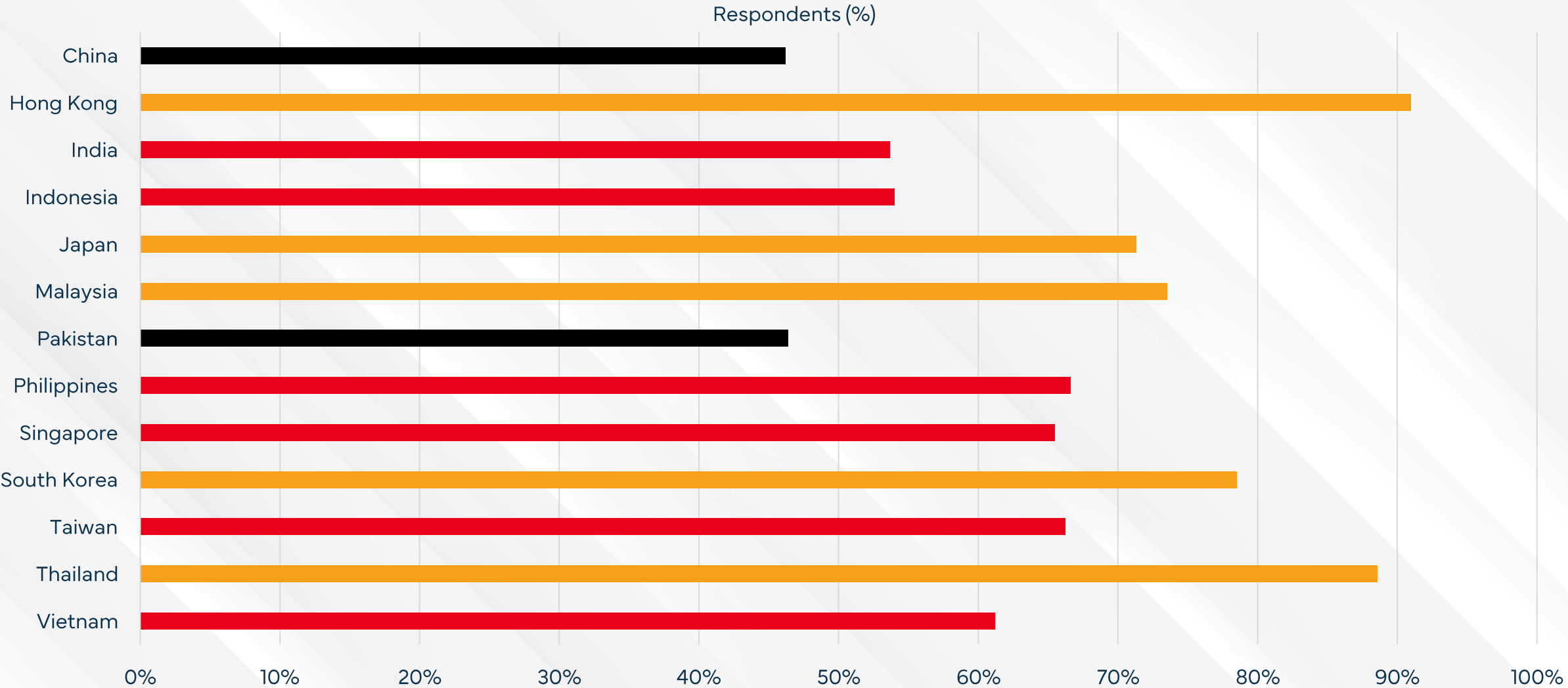Global Anti-Scam Alliance

Respondents (%)

China, India, Indonesia, the Philippines are the most confident in their abilities to recognize scams.

How confident are you that you can recognize scams?
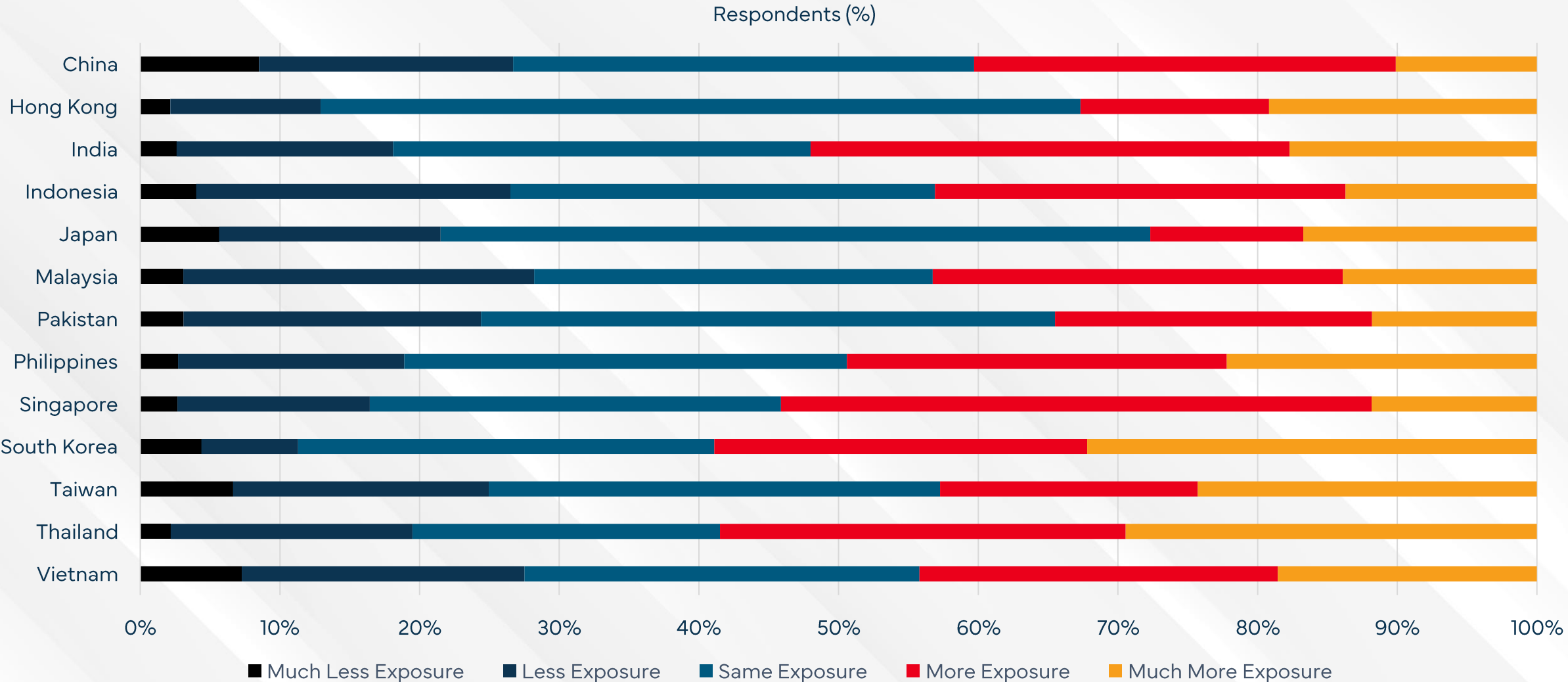
Hong Kong & Thailand face scams most frequently
~90% of citizens encounter scams once per month or more

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Country	Value
China	~46%
Hong Kong	~91%
India	~54%
Indonesia	~54%
Japan	~71%
Malaysia	~73%
Pakistan	~46%
Philippines	~66%
Singapore	~65%
South Korea	~78%
Taiwan	~66%
Thailand	~89%
Vietnam	~61%

0%   10%   20%   30%   40%   50%   60%   70%   80%   90%   100%

Less than half of the Chinese & Pakistani populations experience at least one scam a month.

In the last 12 months, how often have you been exposed to scam attempts? This includes receiving suspicious content, as well as seeing deceitful advertising.

Thailand and South Korea reported the largest increase in scams

Respondents (%)

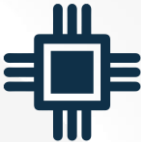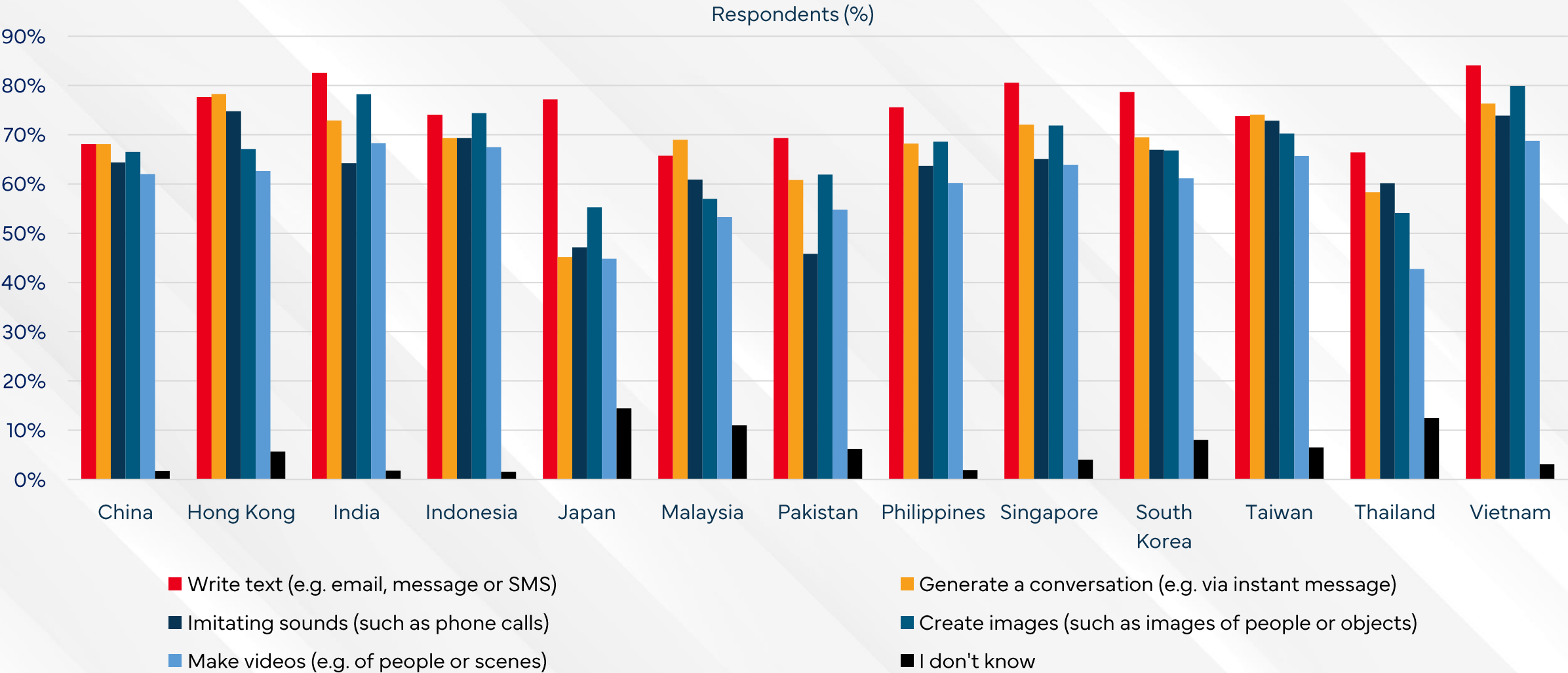| | Much Less Exposure | Less Exposure | Same Exposure | More Exposure | Much More Exposure |

Japan, Hong Kong & Pakistan remained stable, while Vietnam & Malaysia reported largest reductions.

Compared to the year before, do you feel you have been exposed more or less frequently by an individual/company that tried to deceive you in the last 12 months?

Japan, Thailand & Malaysia are least informed about AI threats

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Legend:
- Write text (e.g. email, message or SMS)
- Generate a conversation (e.g. via instant message)
- Imitating sounds (such as phone calls)
- Create images (such as images of people or objects)
- Make videos (e.g. of people or scenes)
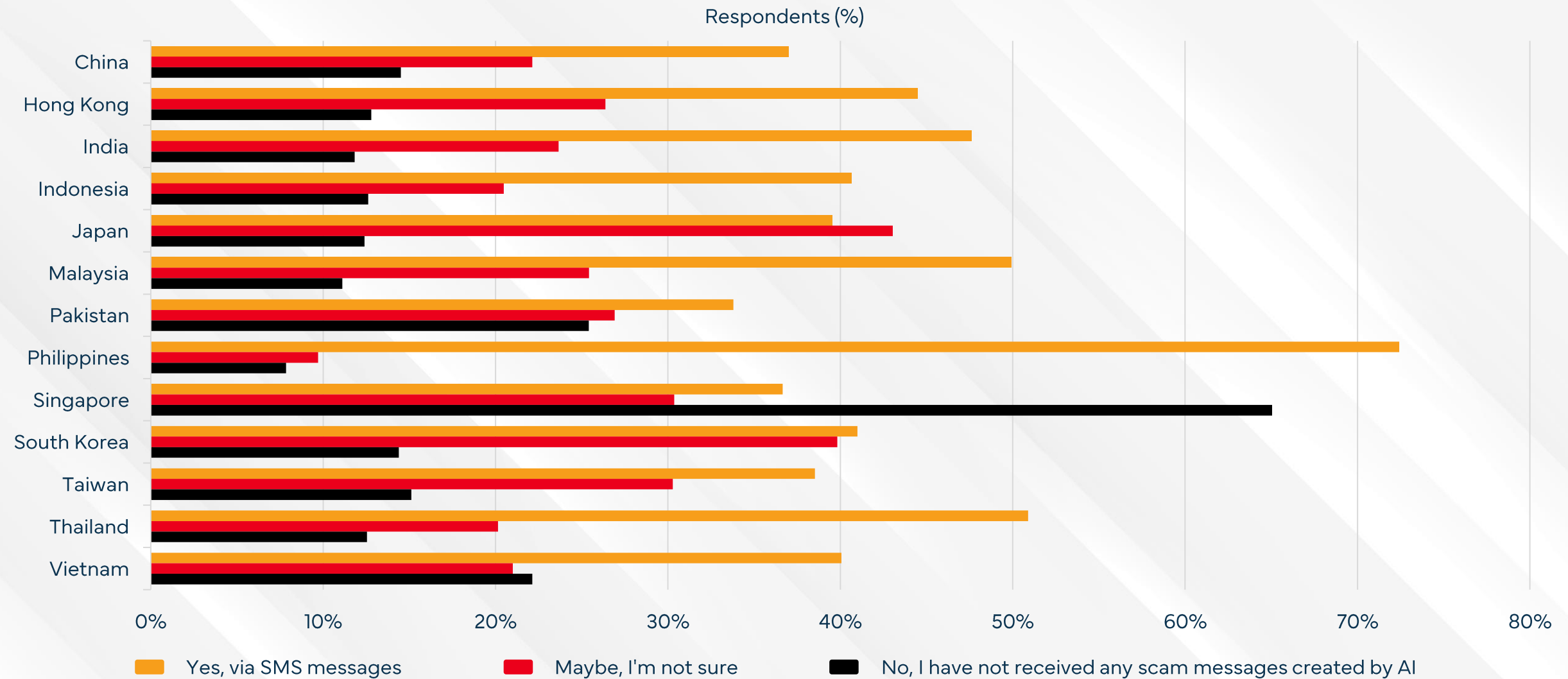- I don't know

The Vietnamese and Indians are the most educated on the wide capabilities of new AI threats.

For which of the following can Artificial Intelligence (AI) be used?

Phone call scams are common in Thailand, Hong Kong, & Malaysia

SCAMADVISER — GASA Global Anti-Scam Alliance

	Email	Social Media	Text/SMS	Chat App	Phone Calls
China					
Hong Kong					
India					
Indonesia					
Japan					
Malaysia					
Pakistan					
Philippines					
Singapore					
South Korea					
Taiwan					
Thailand					
Vietnam					

Text/SMS Messages are common in the Philippines, South Korea, Hong Kong & Indonesia

Through which communication channel(s) did scammers approach you in the last 12 months?

* One block represents 10%

AI SMS scams: 72% of Filipinos believe they have been targeted

Respondents (%)

China
Hong Kong
India
Indonesia
Japan
Malaysia
Pakistan
Philippines
Singapore
South Korea
Taiwan
Thailand
Vietnam

0% 10% 20% 30% 40% 50% 60% 70% 80%

■ Yes, via SMS messages   ■ Maybe, I'm not sure   ■ No, I have not received any scam messages created by AI

The majority of Singaporeans do not believe AI was involved in scams against them.

Do you think Artificial Intelligence (AI) was used in an attempt to scam you?

China
Identity Theft
Shopping
Authority

Japan
Identity Theft
Investment
Advance Fee

Singapore
Identity Theft
Investment
Shopping

Vietnam
Identity Theft
Investment
Authority

Hong Kong
Authority
Identity Theft
Threats & Extortion

Malaysia
Investment
Identity Theft
Shopping

South Korea
Investment
Identity Theft
Employment

Scam Types
- Advance Fee
- Authority
- Charity
- Employment
- Fake Invoice
- Identity Theft
- Investment
- Romance
- Shopping
- Threats & Extortion

India
Shopping
Investment
Employment

Pakistan
Investment
Shopping
Advance Fee

Taiwan
Identity Theft
Shopping
Authority

Indonesia
Investment
Shopping
Charity

Philippines
Shopping
Investment
Identity Theft

Thailand
Identity Theft
Shopping
Fake Invoice

Investment & Shopping scams are rampant across Asia, appearing in the top 3 of several populations.

Which of the following negative experiences happened to you in the last 12 months?

SCAMADVISER

GASA
Global Anti-Scam Alliance

"Received an email from someone who claimed that he had hacked into my computer and camera, took some photos, and threatened me to transfer BTC to the address he provided." (China)
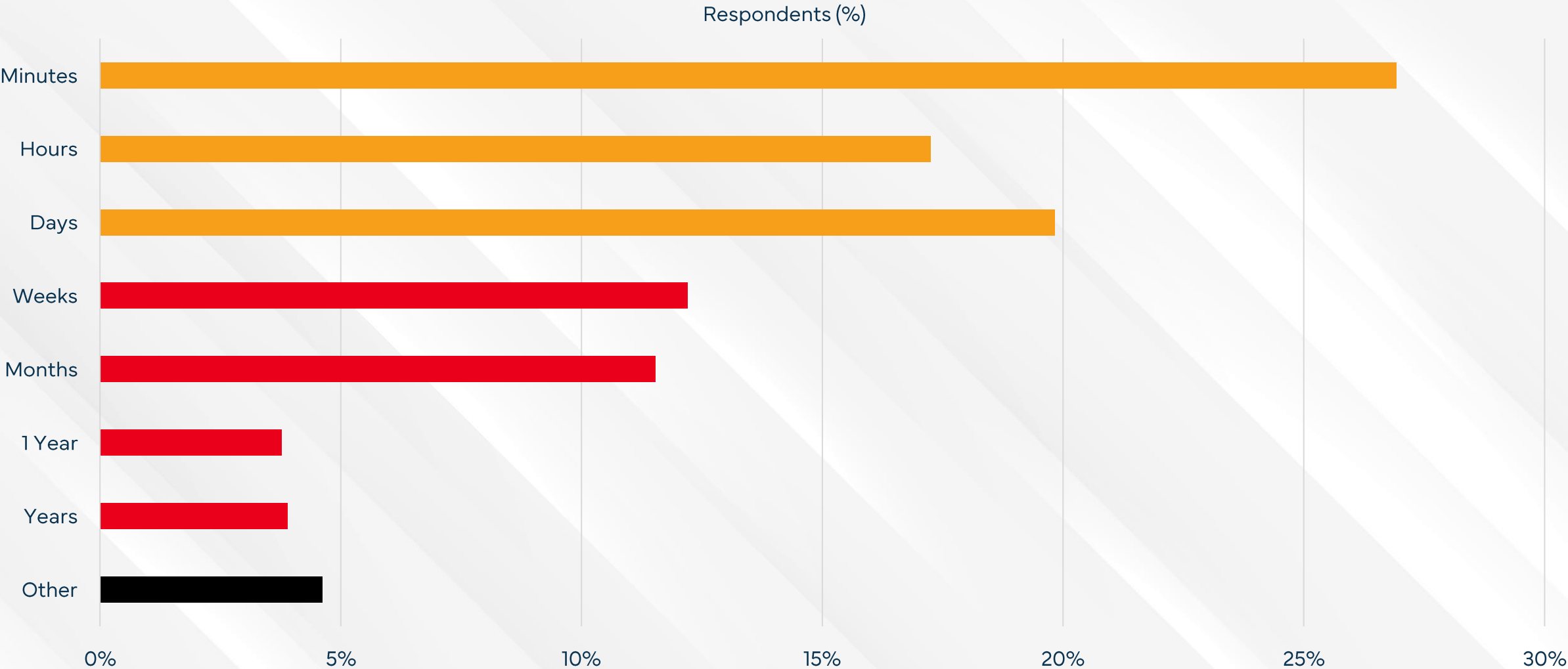
"Ordered items worth Rs.8000/- from a page on Instagram but never received my money back or crockery. They have blocked me and their number is not reachable. I paid through UPI." (India)

"The scammer claimed that I had subscribed to a paid financial instrument service. If I wanted to cancel, I needed to provide the scammer with my personal information and financial status." (Hong Kong)

"I was called by someone who claimed to be a police officer who had arrested my child for hitting a small child to death. To lighten the sentence, the police offered to do it peacefully, on the condition that I transfer 15 million rupiahs... on the pretext that it was to be given to his commander." (Indonesia)

"Scammers often send messages on Facebook and invite you to add them on Line, pretending to flirt, chat, and create hopes of building a future together before tricking you into investing in businesses such as stock trading, playing Bitcoin, etc. In the end, the money invested is not returned." (Thailand)

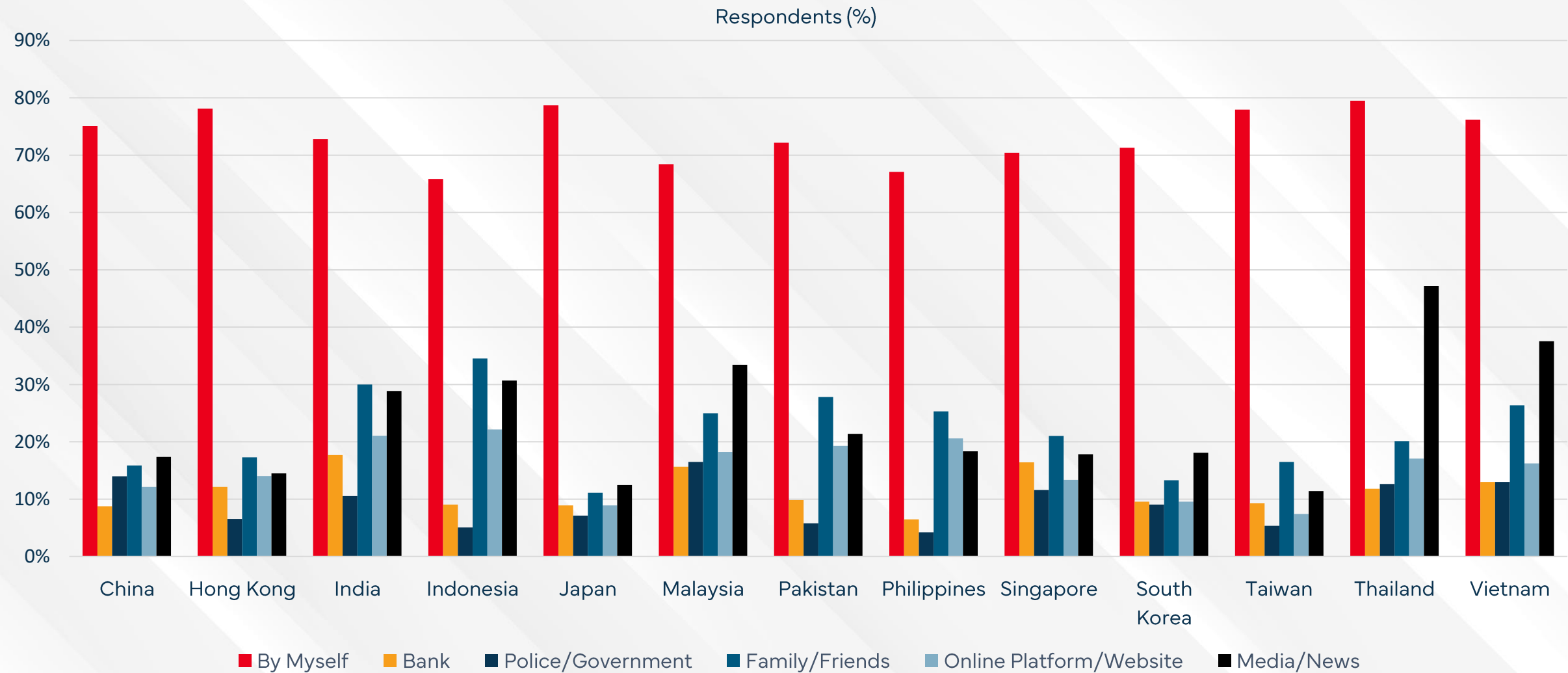# 1-in-4 scams take only a matter of minutes to complete

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Minutes	
Hours	
Days	
Weeks	
Months	
1 Year	
Years	
Other	

0%   5%   10%   15%   20%   25%   30%

8% of Asian scam experiences took place over a year or more.

How long did the scam last, from the first time you heard from the scammer until the last payment you made or the last time you contacted them?
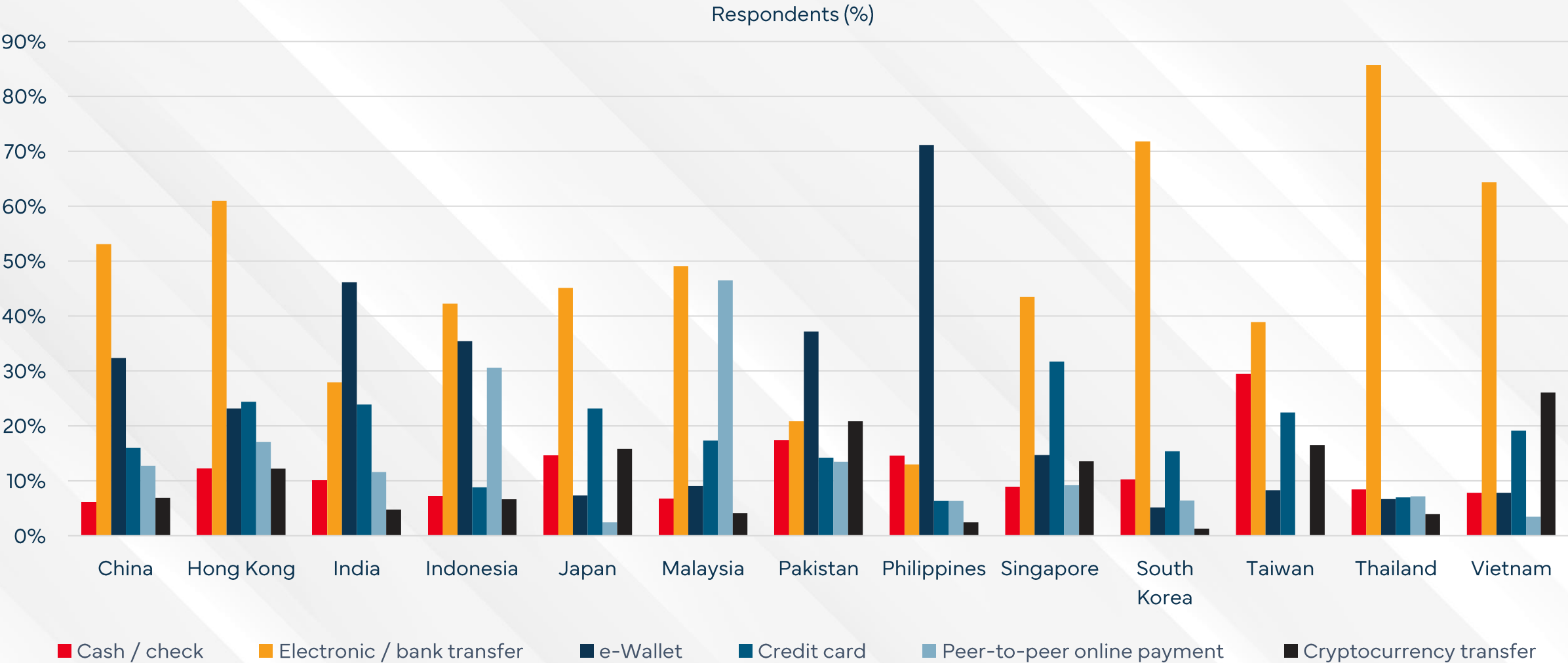
Most Asians are able to come to their own conclusion that they have been scammed

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Legend:
- By Myself
- Bank
- Police/Government
- Family/Friends
- Online Platform/Website
- Media/News

The media/news plays a crucial role in scam awareness, particularly in Thailand and Vietnam.
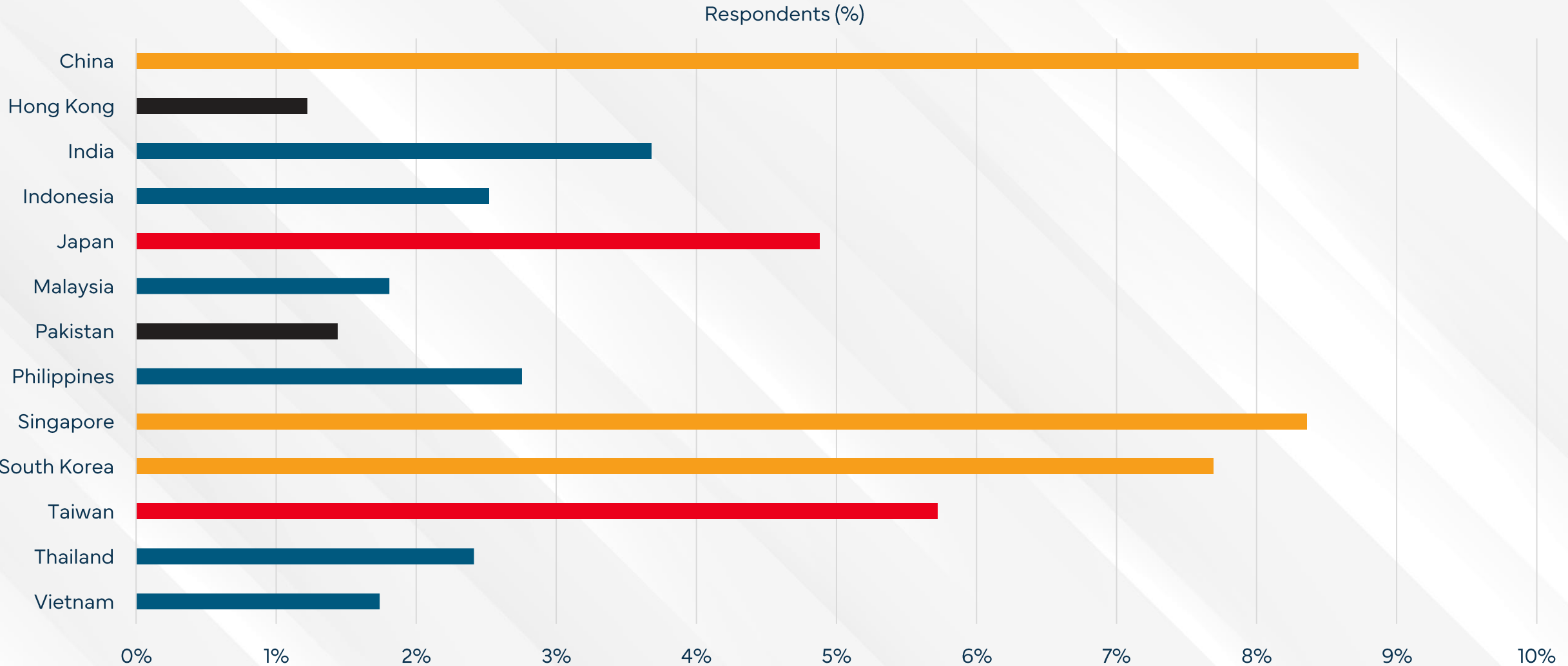
How did you discover you were scammed?

Bank Transfers are Asia's dominant scam payment method

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Cash / check ■ Electronic / bank transfer ■ e-Wallet ■ Credit card ■ Peer-to-peer online payment ■ Cryptocurrency transfer

Electronic transfer & e-Wallets are popular, while cryptocurrency scams have seen a spike in Vietnam.

How did you pay the scammer?

Victims from China, Singapore, and South Korea said that they were more likely to recover their scam losses in full

SCAMADVISER

GASA Global Anti-Scam Alliance

Respondents (%)

Country	
China	
Hong Kong	
India	
Indonesia	
Japan	
Malaysia	
Pakistan	
Philippines	
Singapore	
South Korea	
Taiwan	
Thailand	
Vietnam	

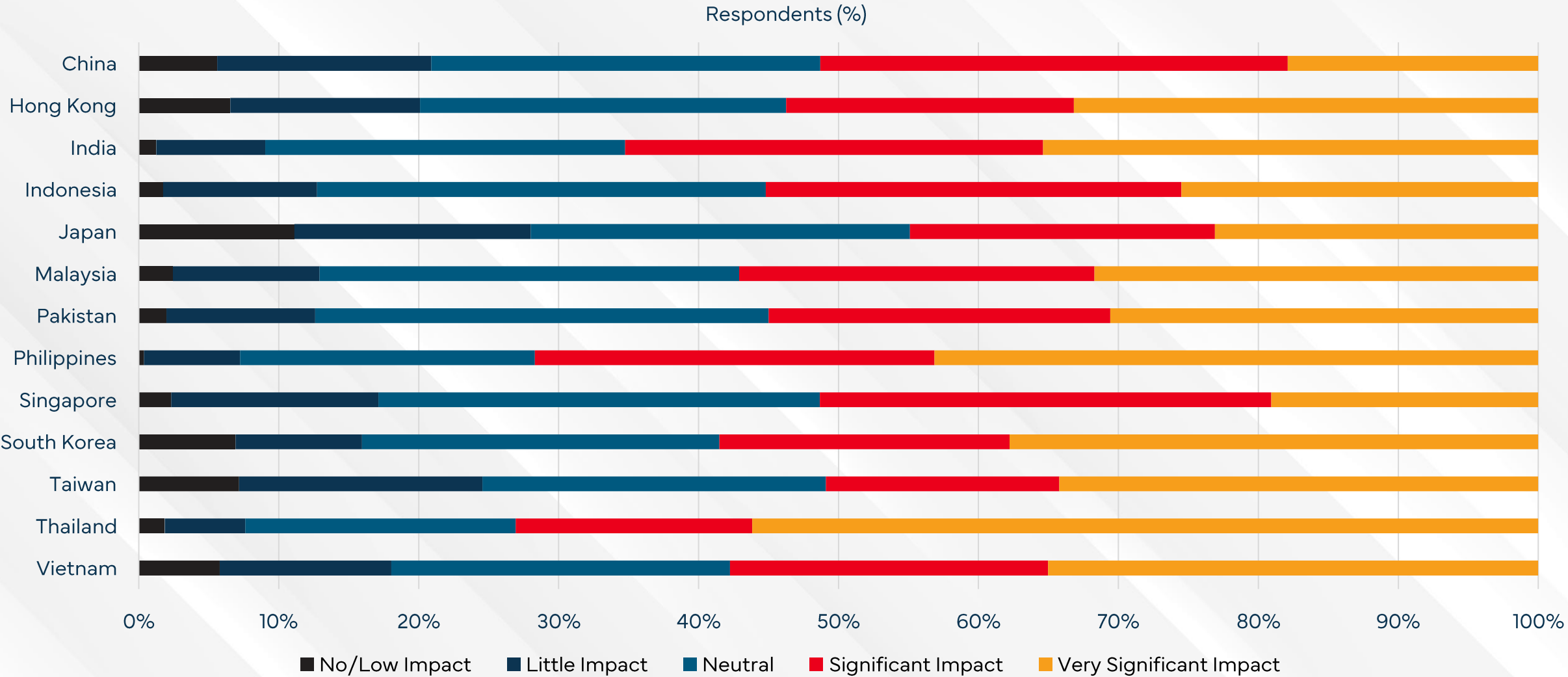0%   1%   2%   3%   4%   5%   6%   7%   8%   9%   10%

Victims from Hong Kong & Pakistan believe they are less likely to recover their losses compared to other Asian populations.

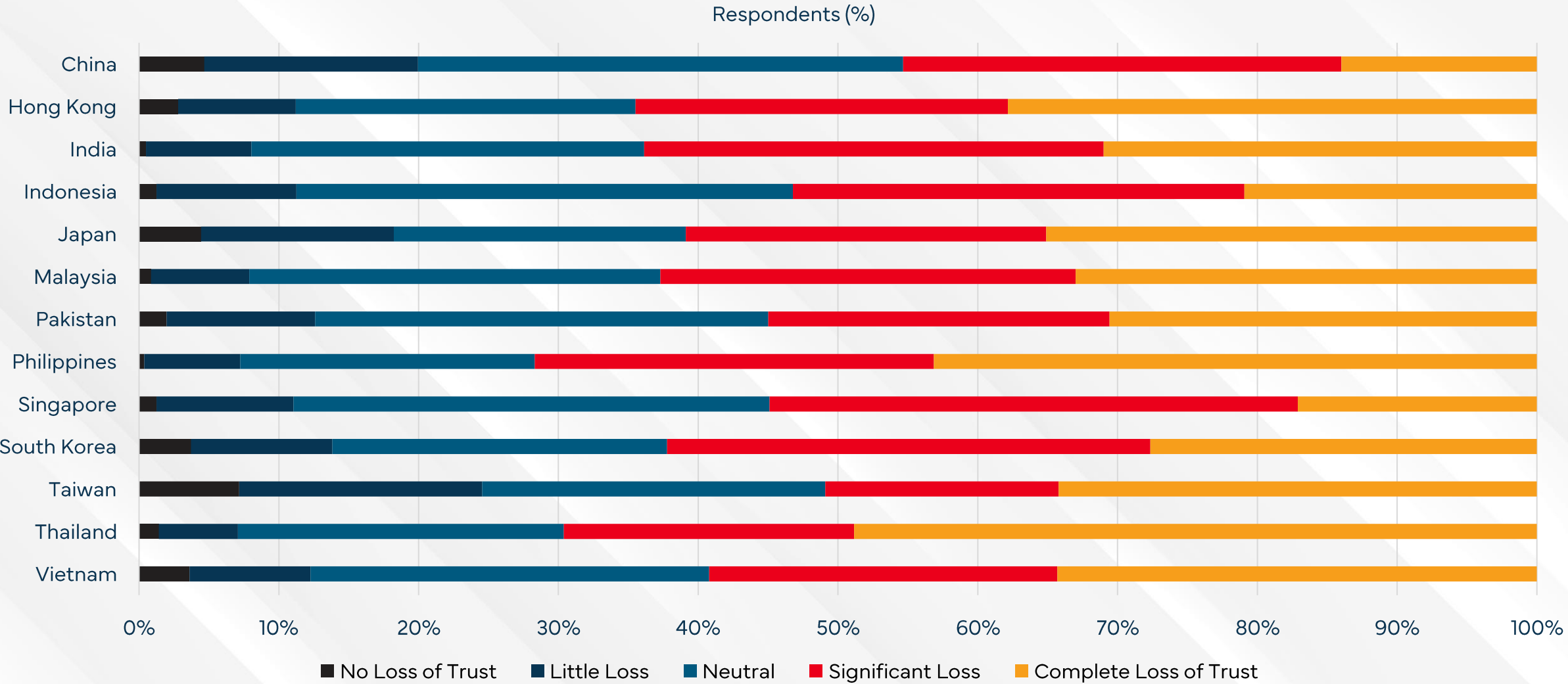Did you try to recover the money lost?

Thai & Filipino scam victims bear the heaviest emotional burden

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Legend: ■ No/Low Impact ■ Little Impact ■ Neutral ■ Significant Impact ■ Very Significant Impact

The Japanese reported the least severe emotional impacts due to scams, followed by Taiwan.

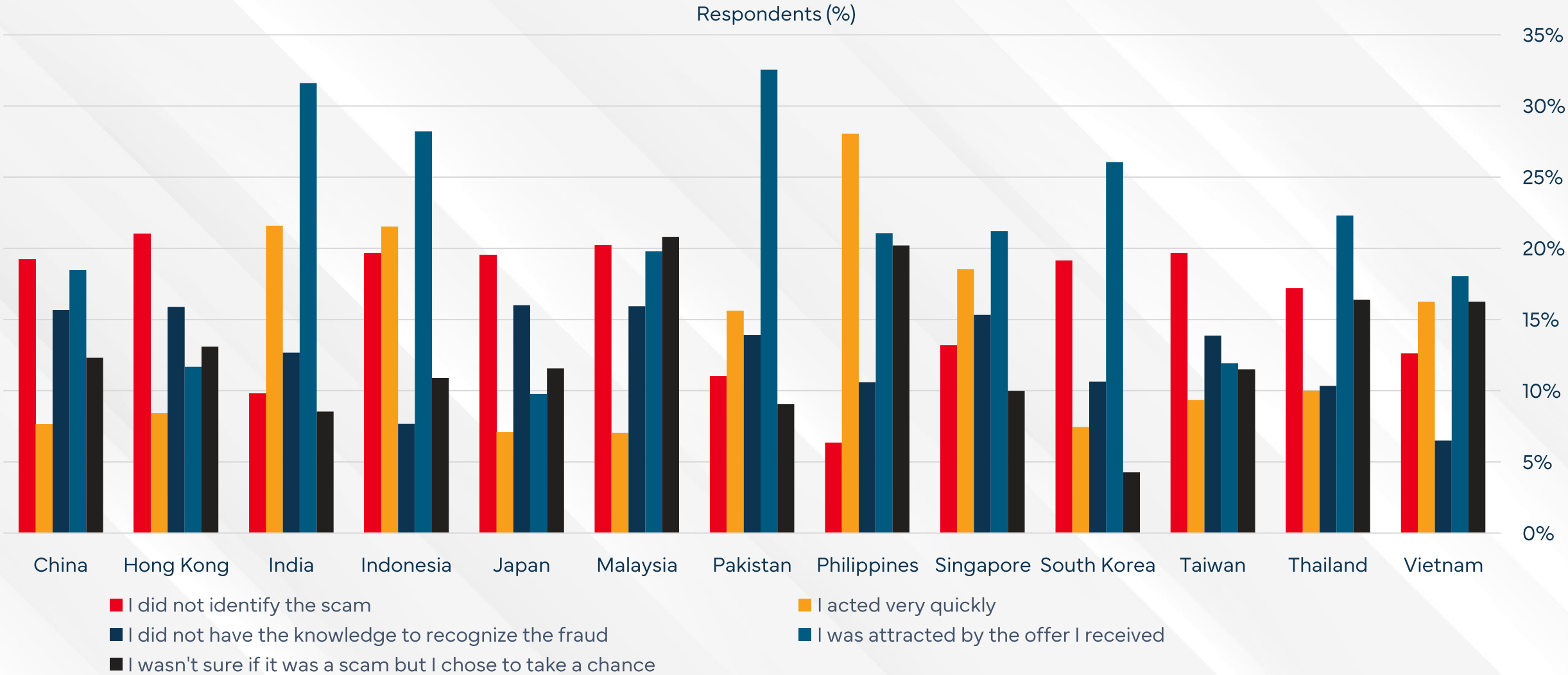To what extent do scams impact your trust in the Internet, in general?

Filipinos & Thais have less in trust the Internet because of scams

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Country	
China	
Hong Kong	
India	
Indonesia	
Japan	
Malaysia	
Pakistan	
Philippines	
Singapore	
South Korea	
Taiwan	
Thailand	
Vietnam	

0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

■ No Loss of Trust   ■ Little Loss   ■ Neutral   ■ Significant Loss   ■ Complete Loss of Trust

China & Taiwan reported the least amount of loss of trust in the Internet due to scams.

To what extent do scams impact your trust in the Internet, in general?

Many Asians are caught out by scammers due to the attractiveness of the offer made
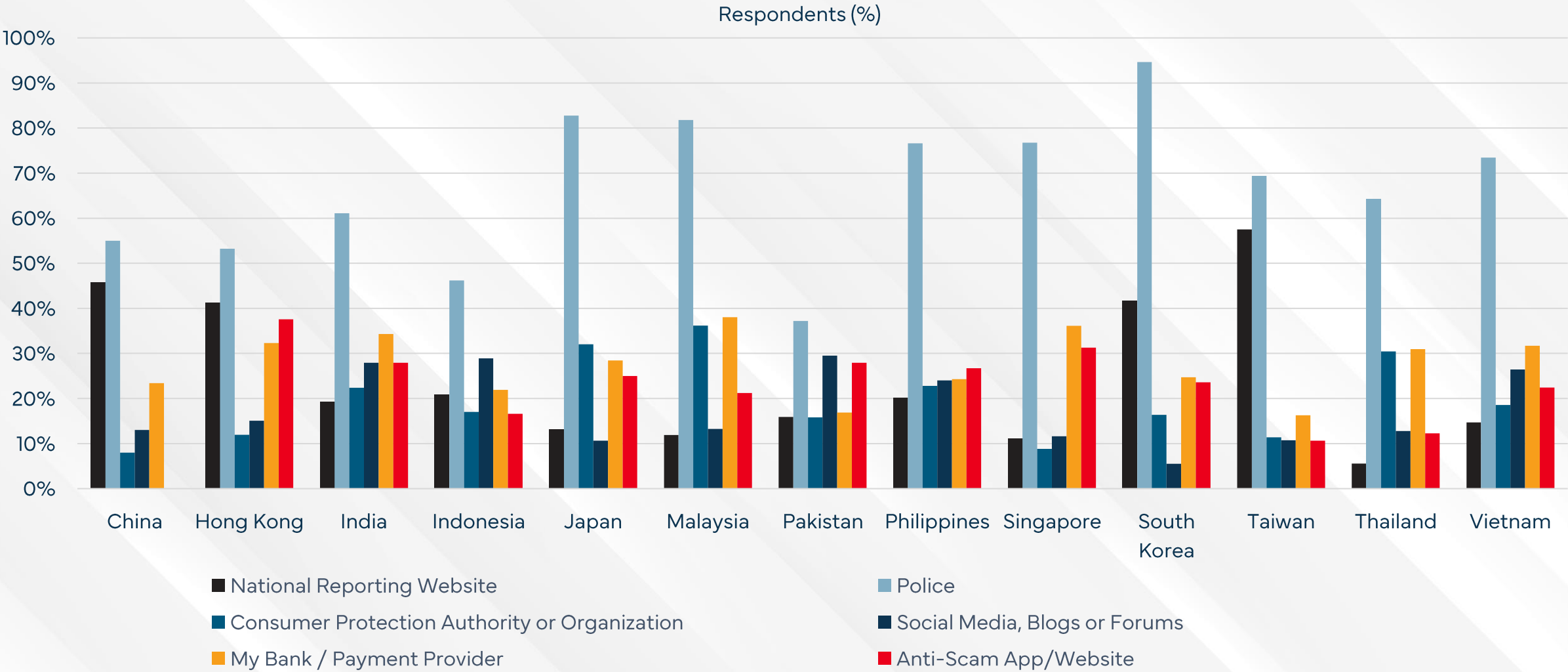
SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Legend:
- I did not identify the scam
- I acted very quickly
- I did not have the knowledge to recognize the fraud
- I was attracted by the offer I received
- I wasn't sure if it was a scam but I chose to take a chance

Countries: China, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Philippines, Singapore, South Korea, Taiwan, Thailand, Vietnam

A sizable portion of victims simply did not detect the scam until it was too late or acted too hastily.

What was the main reason you were deceived?

Police are the main reporting destination for every surveyed Asian country

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

Legend:
- National Reporting Website
- Consumer Protection Authority or Organization
- My Bank / Payment Provider
- Police
- Social Media, Blogs or Forums
- Anti-Scam App/Website

China, Hong Kong, Taiwan, and South Korea have popular National Reporting Websites.

If you were to be deceived by a scam, who would you report this to?

Many Asians don't report scams citing uncertainty where to report

Respondents (%)

Legend:
- Reporting is too complicated (red)
- I don't know who to report it to (orange)
- I fear I won't be believed (dark blue)
- I'm not sure if this is a scam (teal)
- I don't think it's my responsibility to point this out (light blue)
- I think someone else will report it (black)

Countries: China, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Philippines, Singapore, South Korea, Taiwan, Thailand, Vietnam

Others assume it's not their responsibility to report, while others fear they will not be believed.

What reasons might you have to not report a scam?

South Koreans, Indonesians expect the least assistance in scam loss recovery

SCAMADVISER   GASA Global Anti-Scam Alliance

China
Police
Online Platform
Website Provider

Hong Kong
Police
Bank/Payment Prov.
Government

India
Online Platform
Website Provider
Consumer Agency

Indonesia
Website Provider
Online Platform
Consumer Agency

Japan
Website Provider
Online Platform
Banks/Payment Prov.

Malaysia
Online Platform
Financial Supervisory Auth.
Website Provider

Pakistan
Online Platform
Website Provider
No one will refund

Philippines
Online Platform
Website Provider
Consumer Agency

Singapore
Banks/Payment Prov.
Online Platform
No one will refund

South Korea
Online Platform
Website Provider
No one will refund

Taiwan
Online Platform
Website Provider
Banks/Payment Prov.

Thailand
Banks/Payment Prov.
Online Platform
Financial Supervisory Auth.

Vietnam
Police
Banks/Payment Prov.
Consumer Agency

Over a quarter of citizens believe no one will reimburse their scam losses in:
- South Korea
- Indonesia
- Pakistan
- Thailand
- Singapore

The platform used by scammers, website host/provider & banks lead Asians' refund hopes.

If you were scammed, who do you think should be responsible for making sure you are paid back for your loss?

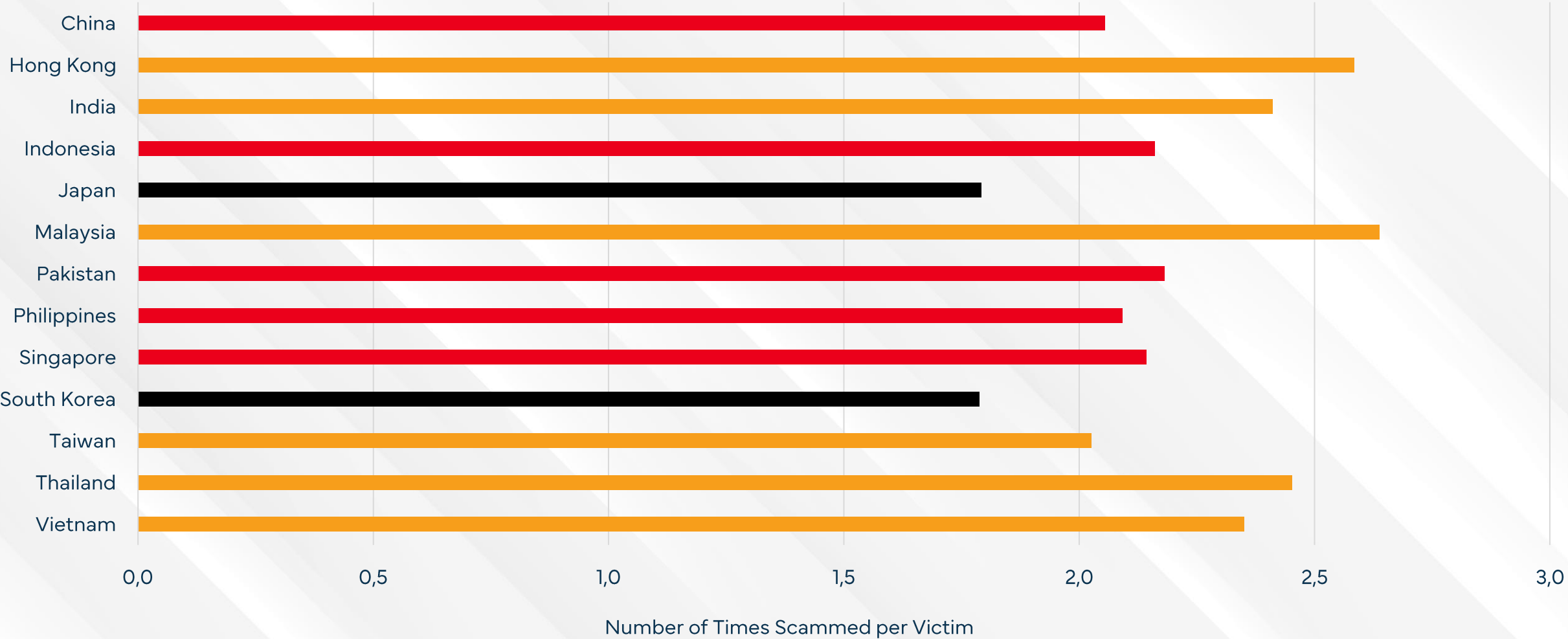# 1-in-5 Indians & Pakistanis admit they may consider money muling

SCAMADVISER

GASA
Global Anti-Scam Alliance

Respondents (%)

The citizens of Taiwan are the least likely to consider taking part in such a fraudulent scheme.

If someone offers you US$ 20,000 on the condition that you send US$ 19,000 to another bank account, leaving you with US$ 1,000 to keep, what would you do?

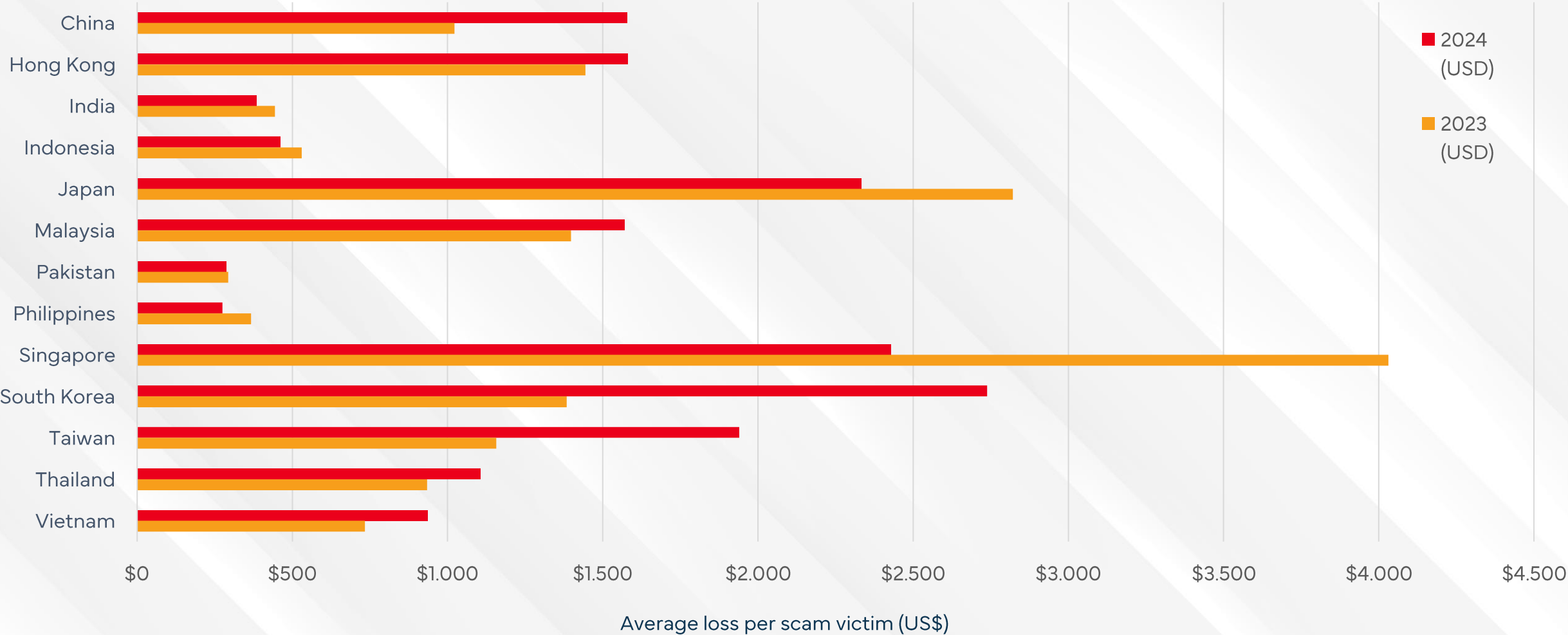# Malaysia & Hong Kong citizens are most likely to be revictimized

Number of Times Scammed per Victim

Country	Value
China	2.05
Hong Kong	2.6
India	2.4
Indonesia	2.15
Japan	1.8
Malaysia	2.65
Pakistan	2.2
Philippines	2.1
Singapore	2.15
South Korea	1.8
Taiwan	2.05
Thailand	2.45
Vietnam	2.35

The citizens of Thailand, India, and Vietnam also highly likely to be retargeted after being scammed.

Which of the following negative experiences happened to you in the last 12 months?

Survey respondents across Asia reported total scam losses of approximately US$688.42 billion

SCAMADVISER **GASA** Global Anti-Scam Alliance

Average loss per scam victim (US$)

Legend:
- **2024 (USD)** (red)
- **2023 (USD)** (orange)

Country	2024 (USD)	2023 (USD)
China	~1,600	~1,020
Hong Kong	~1,600	~1,450
India	~380	~450
Indonesia	~470	~530
Japan	~2,350	~2,800
Malaysia	~1,600	~1,400
Pakistan	~290	~290
Philippines	~270	~360
Singapore	~2,450	~4,050
South Korea	~2,750	~1,400
Taiwan	~1,950	~1,150
Thailand	~1,100	~950
Vietnam	~930	~720

X-axis: $0, $500, $1.000, $1.500, $2.000, $2.500, $3.000, $3.500, $4.000, $4.500

Singapore & Japan reported a drop in scam losses, while South Korea & Taiwan reported significant increases.

In the last 12 months, in total, how much money did you lose to scams before trying to recover the funds?

SCAMADVISER

About
This Report

GASA
Global Anti-Scam Alliance

The **Global Anti-Scam Alliance (GASA)** is a non-profit, bringing together policy makers, law enforcement, consumer authorities, NGOs, the financial sector, cybersecurity, and commercial organizations to share insights and knowledge surrounding scams. GASA releases the annual Global State of Scams report, alongside many secondary reports which focus on the state of scams in various populations.

ScamAdviser is a global leader in scam prevention, committed to empowering businesses with its AI-powered Anti-Scam Intelligence (ASI). Our platform delivers real-time detection of suspicious activities, protecting websites, phone calls, messages, and online platforms from potential scams. With the world's largest scam database, we share insights with 400+ partners, collectively protecting more than 1 billion consumers worldwide.

1. Survey Administration:

- **Tool Used:** Pollfish.com

- **Methodology:** Random Device Engagement (RDE), a successor to Random Digit Dialing (RDD), delivers surveys through popular mobile apps to a neutral, unsuspecting audience. This approach minimizes premeditated survey-taking biases.

2. Incentives and Fraud Prevention:

- **Incentives:** Non-monetary perks, such as extra lives in games or access to premium content.

- **Fraud Prevention:** Advanced AI and machine learning technologies to remove biased responses and enhance data quality.

3. Data Correction and Estimation Challenges:

- **Statistical Corrections:** Adjustments made based on the general demographic distribution within each country to account for potential biases in age or education level.

- **Estimated Amount Lost:** To calculate the total amount lost per country, we followed these steps:
  - Percentage of Participants Losing Money: We first determined the total number of participants who reported losing money in each country. This number was then divided by the total number of survey participants from that country to get the percentage of people who lost money.
  - Estimating the Total Number of Scam Victims: We multiplied the percentage of participants who lost money by the total population over 18 years old in that country. This gave us an estimate of the total number of scam victims in each country.
  - Calculating the Average Amount Lost: The average amount lost per person was calculated by averaging the reported losses from participants in each country, after removing any outliers that could skew the results.
  - Total Money Lost: Finally, we multiplied the estimated total number of scam victims over 18 years old by the average amount lost in their respective country. This provided the estimated total financial loss due to scams for each country.
  - This methodology ensures that the data reflects a reliable estimate of the financial impact of scams across different populations and regions.

- **Estimation Limitations:** Outliers were removed as needed, and losses under one bitcoin were not included due to reporting constraints.

- **Respondents by Country:** China = 1,000; Hong Kong = 511; India = 1,000; Indonesia = 1,000; Japan = 921; Malaysia = 1202; Pakistan = 1,000; Philippines = 1,000; Singapore = 1,109; South Korea = 708; Taiwan = 5,003; Thailand = 9,603; Vietnam = 647. Total Respondents = 24,731. The data presented in this report reflects the responses of each country's participants as percentages of their respective sample sizes. This approach ensures that the insights and trends identified are representative of the surveyed population within each country but are not adjusted to reflect their proportional representation at a regional level. This non-weighted analysis highlights country-specific insights without normalizing for population size differences. It is crucial for readers to consider the unweighted nature of this data when interpreting the results, as it may affect the comparability across different regions with varying sample sizes.

4. Additional Data Sources:

- Inhabitants per country: Worldometers.info
- Currency conversion: Xe.com
- Internet penetration: Wikipedia
- GDP Estimate 2024: Wikipedia

5. Translation and Localization:

- **Procedure:** Each survey was translated and localized by a human to align with the official or most commonly spoken language of the target country.

6. Inspirational Reference:

- **Study:** The methodology was partly inspired by the findings of DeLiema, M., Mottola, G. R., & Deevy, M. (2017) in their pilot study to measure financial fraud in the United States (SSRN 2914560).

SCAMADVISER **GASA** Global Anti-Scam Alliance

Jorij Abraham has been active in the Ecommerce industry since 1997. From 2013 to 2017, he has been Research Director at Thuiswinkel.org, Ecommerce Europe (the Dutch & European Ecommerce Association) and the Ecommerce Foundation.

Nowadays, Jorij is a Professor at TIO University and Managing Director of the Global Anti-Scam Alliance (GASA) & ScamAdviser.

Clement Njoki is Editor and Researcher at GASA. His role involves creating engaging content about scams and fraud, simplifying complex financial information for various platforms. He also works on building GASA's online presence through blogs and news updates.

Clement possesses comprehensive expertise in identifying and combating deceptive practices and fraud, along with a strong background in cybersecurity.

Sam Rogers is GASA's Director of Marketing. Previously, he worked in Risk Advisory, before transitioning into a career as a researcher, copywriter, and content manager specialized in cutting-edge electrical engineering topics, such as photonics and the industrial applications of electromagnetic radiation.

Sam left the world of corporate industry seeking a role which would allow him to concentrate on networking and events management, while allowing him to contribute something worthwhile to society.

James Greening, operating under a pseudonym, brings a wealth of experience to his role as a scam investigator, content writer, and social media manager. Formerly the sole driving force behind Fake Website Buster, James leverages his expertise to raise awareness about online scams. He currently serves as a Content Writer and Social Media Manager for the Global Anti-Scam Alliance (GASA) and regularly contributes to ScamAdviser.com.

INTELLIGENCE SHARING
Regular Virtual Meet-ups
8 Topic-based Email Groups
10,000 Professionals Newsletter

RESEARCH
Global State of Scams
30+ Regional Reports
Policy Papers

NETWORKING
3 International Summits
Online Member Directory
National GASA Chapters

CYBERCRIME EXCHANGE
80+ Pooled Data Sources
Realtime Data Sharing
Access to Global Leaderboards

OUR FOUNDATION PARTNERS

Become a member, see all member benefits at: gasa.org/membership